

**PEMBANGUNAN MODEL PROTOKOL KEAMANAN
PADA SISTEM RESEP ELEKTRONIK MENGGUNAKAN
*DIGITAL SIGNATURE ALGORITHM (DSA)***

SKRIPSI

Diajukan untuk Memenuhi Sebagian dari
Syarat Memperoleh Gelar Sarjana Komputer
Program Studi Ilmu Komputer



oleh:
IRA YUSTIANA NABILA
1401493

**PROGRAM STUDI ILMU KOMPUTER
DEPARTEMEN PENDIDIKAN ILMU KOMPUTER
FAKULTAS PENDIDIKAN MATEMATIKA DAN
ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA**

Ira Yustiana Nabila, 2019

***PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK
MENGGUNAKAN DIGITAL SIGNATURE ALGORITHM (DSA)***

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

2019
**PEMBANGUNAN MODEL PROTOKOL KEAMANAN
PADA SISTEM RESEP ELEKTRONIK MENGGUNAKAN
*DIGITAL SIGNATURE ALGORITHM (DSA)***

Oleh
Ira Yustiana Nabila

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat
memperoleh gelar Sarjana pada Fakultas Pendidikan Matematika dan
Ilmu Pengetahuan Alam

© Ira Yustiana Nabila 2019

Universitas Pendidikan Indonesia

2019

Hak cipta dilindungi undang-undang
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,
Dengan dicetak ulang, difoto kopi, atau
cara lainnya tanpa ijin dari penulis

Ira Yustiana Nabila, 2019

***PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK
MENGGUNAKAN DIGITAL SIGNATURE ALGORITHM (DSA)***

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

IRA YUSTIANA NABILA

1401493

**PEMBANGUNAN MODEL PROTOKOL KEAMANAN
PADA SISTEM RESEP ELEKTRONIK MENGGUNAKAN
*DIGITAL SIGNATURE ALGORITHM (DSA)***

DISETUJUI DAN DISAHKAN OLEH PEMBIMBING:
Pembimbing I,

Rizky Rachman J.Putra, M.Kom.
NIP. 197711252006041002

Pembimbing II,

Jajang Kusnendar, M.T.
NIP. 198903252015041001

Mengetahui,
Ketua Departemen Pendidikan Ilmu Komputer,

Ira Yustiana Nabila, 2019

**PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK
MENGGUNAKAN DIGITAL SIGNATURE ALGORITHM (DSA)**

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

Prof. Dr. H. Munir, M.IT
NIP. 19660325200112100

Ira Yustiana Nabila, 2019

***PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK
MENGUNAKAN DIGITAL SIGNATURE ALGORITHM (DSA)***

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul “Pembangunan Model Protokol Keamanan Pada Sistem Resep Elektronik Menggunakan *Digital Signature Algorithm* (DSA)” ini sepenuhnya karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung sanksi apabila ditemukan adanya pelanggaran terhadap etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya ini.

Bandung, Januari 2019
Pembuat Pernyataan,

Ira Yustiana Nabila
NIM. 1401493

Ira Yustiana Nabila, 2019

**PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK
MENGUNAKAN DIGITAL SIGNATURE ALGORITHM (DSA)**

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

PADA SISTEM RESEP ELEKTRONIK MENGGUNAKAN *DIGITAL SIGNATURE ALGORITHM* (DSA)

Oleh

Ira Yustiana Nabila — irayustiananabila@student.upi.edu

1401493

ABSTRAK

Bidang kesehatan merupakan bidang yang sangat mungkin untuk diintegrasikan dengan adanya teknologi informasi, salah satunya pada sistem resep elektronik. Digitalisasi resep merupakan salah satu alat yang paling efektif untuk mengurangi kesalahan pengobatan serta penyalahgunaan obat tanpa resep dokter. Namun terdapat masalah yang timbul dari pengelolaan program melalui internet yaitu mengenai kerahasiaan, otentikasi keaslian tanda tangan dan integritas data dari resep elektronik. Hal tersebut dapat diatasi dengan menggunakan teknik kriptografi, salah satunya dengan menggunakan metode *digital signature algorithm* yang dikhususkan untuk tanda tangan digital. Sistem resep elektronik ini menggunakan *digital signature algorithm* untuk proses pembentukan tanda tangan dan verifikasi demi keamanan informasi, integritas data, otentikasi serta mencegah modifikasi dan akses tidak sah. Aspek kriptografi diharapkan untuk memastikan file resep pada identitas, pemeriksaan dan layanan yang diberikan benar untuk pasien atau orang yang berwenang. Dari hasil pengujian skenario *man in the middle attack* pada resep elektronik ini menunjukkan bahwa 6 dari hasil pengujian resep dengan menggunakan *digital signature algorithm* dapat memberikan jaminan otentikasi pengirim dan penerima, serta dapat menjaga integritas data.

Kata Kunci: Resep Obat, Kriptografi, Tanda Tangan Digital, *Digital Signature Algorithm*.

Ira Yustiana Nabila, 2019

**PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK
MENGGUNAKAN *DIGITAL SIGNATURE ALGORITHM* (DSA)**

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

THE DEVELOP OF A SECURITY PROTOCOL MODEL ON ELECTRONIC PRESCRIPTION SYSTEMS USING A DIGITAL SIGNATURE ALGORITHM (DSA)

Oleh

Ira Yustiana Nabila — irayustiananabila@student.upi.edu

1401493

ABSTRACT

The health sector can be very possible to be integrated with the existence of information technology. For the example, electronic prescription system. Digitalization recipes is one of the most effective tools to reduce medication errors and drug abuse without a prescription. However, there are problems that come from managing programs through the internet, there are regarding confidentiality, authentication of authenticity of signatures and integrity of data from electronic prescriptions. This matters can be solved by using cryptographic techniques, one of which is by using the digital signature algorithm method specifically for digital signatures. The electronic prescription system using a digital signature algorithm for the process of forming signatures and verification for information security, data integrity, authentication and preventing unauthorized modification and validity access. Cryptographic aspects are expected to ensure that prescription files on identity, inspection and services provided are correct for patients or authorized persons. The results of testing on electronic recipes show that the digital signature algorithm can guarantee the authenticity of senders and recipients, and can maintain data integrity. From the results of testing '*man in the middle attack*' on electronic prescriptions it proves that 6 from the test results of the prescription results using a digital signature algorithm can provide guaranteed payments and recipients, and can secure the data.

Ira Yustiana Nabila, 2019

**PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK
MENGUNAKAN DIGITAL SIGNATURE ALGORITHM (DSA)**

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

Keywords: Prescription, Cryptographi, Digital Signature, Digital Signature Algorithm.

Ira Yustiana Nabila, 2019

***PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK
MENGUNAKAN DIGITAL SIGNATURE ALGORITHM (DSA)***

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

DAFTAR ISI

| | |
|--|-------------------------------------|
| PERNYATAAN | vii |
| KATA PENGANTAR | Error! Bookmark not defined. |
| UCAPAN TERIMA KASIH..... | Error! Bookmark not defined. |
| ABSTRAK..... | viii |
| <i>ABSTRACT</i> | ix |
| DAFTAR ISI..... | xi |
| DAFTAR TABEL..... | i |
| DAFTAR GAMBAR | ii |
| BAB I PENDAHULUAN | Error! Bookmark not defined. |
| 1.1 Latar Belakang..... | Error! Bookmark not defined. |
| 1.2 Rumusan Masalah | Error! Bookmark not defined. |
| 1.3 Tujuan Penelitian..... | Error! Bookmark not defined. |
| 1.4 Batasan Masalah | Error! Bookmark not defined. |
| 1.5 Sistematika Penulisan Skripsi..... | Error! Bookmark not defined. |
| BAB II KAJIAN PUSTAKA | Error! Bookmark not defined. |
| 2.1 Sistem Informasi Kesehatan . | Error! Bookmark not defined. |
| 2.2 Rekam Medis..... | Error! Bookmark not defined. |
| 2.3 Resep Obat | Error! Bookmark not defined. |
| 2.3.1 Resep | Error! Bookmark not defined. |
| 2.3.2 Resep Elektronik..... | Error! Bookmark not defined. |
| 2.4 Kriptografi | Error! Bookmark not defined. |
| 2.4.1 Definisi Kriptografi | Error! Bookmark not defined. |
| 2.4.2 Tujuan Kriptografi | Error! Bookmark not defined. |
| 2.4.3 Konsep Dasar Kriptografi | Error! Bookmark not defined. |
| 2.4.4 Komponen Kriptografi. | Error! Bookmark not defined. |
| 2.5 Tanda Tangan Digital (<i>Digital Signature</i>). | Error! Bookmark not defined. |
| 2.5.1 <i>Digital Signature Algorithm (DSA)</i> ... | Error! Bookmark not defined. |
| 2.5.2 Fungsi <i>Hash</i> (SHA) | Error! Bookmark not defined. |

Ira Yustiana Nabila, 2019

**PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK
MENGUNAKAN DIGITAL SIGNATURE ALGORITHM (DSA)**

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

| | | |
|--|---|-------------------------------------|
| 2.6 | <i>Quick Response Code (QR Code)</i> | Error! Bookmark not defined. |
| BAB III METODE PENELITIAN..... Error! Bookmark not defined. | | |
| 3.1 | Desain Penelitian | Error! Bookmark not defined. |
| 3.1.1 | Tahap Awal Penelitian. | Error! Bookmark not defined. |
| 3.1.2 | Studi Literatur | Error! Bookmark not defined. |
| 3.1.3 | Analisis dan Rancangan Sistem . | Error! Bookmark not defined. |
| 3.1.4 | Testing | Error! Bookmark not defined. |
| 3.1.5 | Dokumentasi | Error! Bookmark not defined. |
| 3.2 | Metode Penelitian | Error! Bookmark not defined. |
| 3.2.1 | Metode Pengumpulan Data..... | Error! Bookmark not defined. |
| 3.2.2 | Metode Pengembangan Perangkat Lunak | Error! Bookmark not defined. |
| 3.3 | Alat dan Bahan Penelitian | Error! Bookmark not defined. |
| 3.3.1 | Alat Penelitian | Error! Bookmark not defined. |
| 3.3.2 | Bahan Penelitian | Error! Bookmark not defined. |
| BAB IV HASIL PENELITIAN DAN PEMBAHASAN Error! Bookmark not defined. | | |
| 4.1 | Hasil Penelitian..... | Error! Bookmark not defined. |
| 4.2 | Perancangan Protokol Resep Elektronik.... | Error! Bookmark not defined. |
| 4.3 | Pengembangan Perangkat Lunak..... | Error! Bookmark not defined. |
| 4.3.1 | Deskripsi sistem | Error! Bookmark not defined. |
| 4.3.2 | Batasan Perangkat Lunak..... | Error! Bookmark not defined. |
| 4.3.3 | Proses Operasional Perangkat Lunak | Error! Bookmark not defined. |
| 4.3.4 | Pengujian | Error! Bookmark not defined. |
| 4.4 | Implementasi <i>Digital Signature Algorithm (DSA)</i> | Error! Bookmark not defined. |
| 4.4.1 | Proses Pembentukan Tanda tangan... | Error! Bookmark not defined. |

| | | |
|----------------------------|--|-------------------------------------|
| 4.4.2 | Proses Verifikasi | Error! Bookmark not defined. |
| 4.5 | Pembahasan Proses Keamanan Otentikasi Sistem Resep | Error! Bookmark not defined. |
| 4.5.1 | Pembangkitan Sepasang Kunci.. | Error! Bookmark not defined. |
| 4.5.2 | Prosedur Pembangkitkan Tanda Tangan..... | Error! Bookmark not defined. |
| 4.5.3 | Proses Verifikasi Keabsahan Tanda Tangan..... | Error! Bookmark not defined. |
| 4.6 | Pengujian <i>Man In The Middle Attack</i> . | Error! Bookmark not defined. |
| 4.7 | Hasil Penelitian..... | Error! Bookmark not defined. |
| BAB V KESIMPULAN DAN SARAN | | Error! Bookmark not defined. |
| 5.1 | Kesimpulan..... | Error! Bookmark not defined. |
| 5.2 | Saran | Error! Bookmark not defined. |
| DAFTAR PUSTAKA | | iii |

DAFTAR TABEL

Tabel 2.1 Fungsi Hash (Maryanto, 2008)..... **Error! Bookmark not defined.**

Tabel 2.2 Kapasitas Koreksi Kesalahan QR Code **Error! Bookmark not defined.**

Tabel 4.1 Pengujian man in the middle attack dengan foto QR Code **Error! Bookmark not defined.**

Tabel 4.2 Pengujian man in the middle attack dengan cetak QR Code **Error! Bookmark not defined.**

Tabel 4.3 Pengujian man in the middle attack dengan foto QR Code berbeda..... **Error! Bookmark not defined.**

Tabel 4.4 Pengujian man in the middle attack dengan foto QR Code berbeda..... **Error! Bookmark not defined.**

DAFTAR GAMBAR

Gambar 2.1 Contoh Resep Dokter (Amalia & Sukohar, 2014) ... **Error! Bookmark not defined.**

Gambar 2.2 Contoh Penerapan Resep Dalam Sistem **Error! Bookmark not defined.**

Gambar 2.3 Skema Proses Digital Signature..... **Error! Bookmark not defined.**

Gambar 2.4 Grafik Perbandingan DSA dan RSA) **Error! Bookmark not defined.**

Gambar 2.5 Contoh QR Code (A. Rahmawati & Rahman, 2011) **Error! Bookmark not defined.**

Gambar 3.1 Desain Penelitian **Error! Bookmark not defined.**

Gambar 3.2 Model Waterfall (Sumber Sommerville, 2011) **Error! Bookmark not defined.**

Gambar 4.1 Rancangan Proses Bisnis Model Protokol Resep **Error! Bookmark not defined.**

Gambar 4.2 Skema Protokol Model Keamanan Resep..... **Error! Bookmark not defined.**

Gambar 4.3 Skema Protokol Model Keamanan Resep..... **Error! Bookmark not defined.**

Gambar 4.4 Alur Proses Pembentukan Tanda Tangan **Error! Bookmark not defined.**

Gambar 4.5 Kode Program Pembentukan Tanda Tangan Digital **Error! Bookmark not defined.**

Gambar 4.6 Alur Proses Verifikasi Pesan **Error! Bookmark not defined.**

Gambar 4.7 Kode Program Verifikasi Pesan..... **Error! Bookmark not defined.**

Gambar 4.8 Memindai QR Code dari resep yang diberikan dokter
..... **Error! Bookmark not defined.**

Gambar 4.9 Hasil Generate QR Code yang baru **Error! Bookmark not defined.**

Gambar 4.10 Proses Scan di Apotek Dengan Sistem Resep **Error! Bookmark not defined.**

Gambar 4.11 Memindai QR Code dari resep lama.... **Error! Bookmark not defined.**

Gambar 4.12 Hasil Generate QR Code baru pada web **Error! Bookmark not defined.**

Gambar 4.13 Proses Scan di Apotek Dengan Sistem **Error! Bookmark not defined.**

DAFTAR PUSTAKA

- Amalia, D. T., & Sukohar, A. (2014). Rational drug prescription writing. *Juke Unila*, 4(01).
- Ardwiansyah, B. (2017). KEABSAHAN PENGGUNAAN TANDA TANGAN ELEKTRONIK SEBAGAI ALAT BUKTI MENURUT UNDANG--UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *LEX PRIVATUM*, 5(7).
- Arifin, S., & Dirgahayu, T. (2018). Evaluasi Implementasi Modul E-Prescribing Rumah Sakit dengan Metode Pieces. *JUITA: Jurnal Informatika*, 5(2), 115–130.
- Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Penerbit Andi.
- Aspden, P., Wolcott, J. A., Bootman, J. L., Cronenwett, L. R., & others. (2007). *Preventing medication errors*. National Academies Press Washington, DC.
- Bell, D. S., Cretin, S., Marken, R. S., & Landman, A. B. (2004). A conceptual framework for evaluating outpatient electronic prescribing systems based on their functional capabilities. *Journal of the American Medical Informatics Association*, 11(1), 60–70.
- Cohen M. R-MS.FASHP, 1999, Medical Errors, American Pharmaceutical Association, Washington DC.
- Dharma, D. (2009). Studi Perbandingan Penggunaan Algoritma Hash SHA 256 dengan Simetrik dan Asimetrik Ciphers dalam Perancangan Secure SWF Rich Internet Application (RIA). Teknik Informatika, Sekolah Teknik Elektro dan Informatika.
- Farida, S., Krisnamurti, D. G. B., Hakim, R. W., Dwijayanti, A., & Purwaningsih, E. H. (2018). Implementasi Peresepan Elektronik. *eJournal Kedokteran Indonesia*, 211-16.
- Hahn, A., & Lovett, A. (2014). Electronic prescribing: an examination of cost effectiveness, clinician adoption and limitations. *Universal Journal of Clinical Medicine*, 2(1), 1–24.

Ira Yustiana Nabila, 2019

PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK MENGGUNAKAN DIGITAL SIGNATURE ALGORITHM (DSA)

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

- Handiwidjojo, W. (2015). Rekam Medis Elektronik. *Jurnal Eksplorasi Karya Sistem Informasi Dan Sains*, 2(1).
- Maryanto, B. (2008). Penggunaan Fungsi Hash Satu Arah Untuk Enkripsi Data. *Jurnal, Informatika, STMIK LIKMI, Bandung*.
- Munir, R. (2006). Kriptografi. *Informatika, Bandung*.
- Pajčin, B. R., & Ivaniš, P. N. (2011). Analysis of Software Realized DSA Algorithm for Digital Signature. *Guest Editorial W*, 73.
- Pratiwi, A. A., & Sinuraya, R. K. (2014). Analisis Peresepan Obat Anak Usia 2--5 Tahun di Kota Bandung Tahun 2012. *Indonesian Journal of Clinical Pharmacy*, 3(1), 18–23.
- Pratiwi, P. S., & Lestari, A. (2012). E-Prescribing: Studi Kasus Perancangan dan Implementasi Sistem Resep Obat Apotik Klinik. *Speed-Sentra Penelitian Engineering Dan Edukasi*, 12(1).
- Purnama, B. E., & Winarko, E. (n.d.). Pengamanan Sistem Data Medis Menggunakan Pola Kriptografi.
- Rahmawati, A., & Rahman, A. (2011). Sistem Pengamanan Keaslian Ijasah Menggunakan QR-Code dan Algoritma Base64. *Program Studi Sistem Informasi, Universitas Ahmad Dahlan*.
- Rahmawati, F., & Oetari, R. A. (2002). Kajian penulisan resep: Tinjauan aspek legalitas dan kelengkapan resep di Apotek-apotek Kotamadya Yogyakarta. *Majalah Farmasi Indonesia*, 13(2), 86–94.
- Reeves, D. (2007). The 2005 Garrod Lecture: The changing access of patients to antibiotics--for better or worse? *Journal of Antimicrobial Chemotherapy*, 59(3), 333–341.
- Salmon, J. W., & Jiang, R. (2012). E-prescribing: history, issues, and potentials. *Online Journal of Public Health Informatics*, 4(3).
- Schneier, B., & others. (1996). Applied cryptography-protocols, algorithms, and source code in C. Wiley New York.
- Sligo, J., Gauld, R., Roberts, V., & Villa, L. (2017). A literature review for large-scale health information system project planning,

Ira Yustiana Nabila, 2019

PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK MENGGUNAKAN DIGITAL SIGNATURE ALGORITHM (DSA)

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

- implementation and evaluation. *International Journal of Medical Informatics*, 97, 86–97.
- Sommerville, I. (2011). Software engineering 9th Edition. *ISBN-10, 137035152*.
- Stalling, J. (2011). *Poetics of Emptiness: Transformations of Asian Thought in American Poetry*. Oxford University Press.
- Talbot, J., Welsh, D., & Welsh, D. J. A. (2006). *Complexity and cryptography: an introduction* (Vol. 13). Cambridge University Press.
- Viktil, K. K., Blix, H. S., Moger, T. A., & Reikvam, A. (2007). Polypharmacy as commonly defined is an indicator of limited value in the assessment of drug-related problems. *British Journal of Clinical Pharmacology*, 63(2), 187–195.
- Wang, L., Wang, Y., Jin, S., Wu, Z., Chin, D. P., Koplan, J. P., & Wilson, M. E. (2008). Emergence and control of infectious diseases in China. *The Lancet*, 372(9649), 1598–1605.
- Winter Nick. *Scan Me: Everybody's Guide to the Magical World of QR Codes*. United States of America: Westsong. 2011.